PRIVACY 101: Orientation Training for all Military Members, Civilian Employees, and Contractor Personnel

What is the Privacy Act (PA)?

- The Privacy Act is a Federal Law that limits an agency's collection and sharing of personal data. The Privacy Act requires that all Executive Branch Agencies follow certain procedures when:
  - Collecting personal information
  - Creating databases containing personal identifiers
  - Maintaining databases containing personal identifiers
  - Disseminating information containing personal data

What are some examples of Privacy Data (Privacy Act/PPI)?

- **Personal data about individuals, such as:**
  - **Social security number, and date of birth**
  - **Financial, credit, and medical data**
  - **Security clearance level**
  - **Leave balances; types of leave used**
  - **Home address and telephone numbers (including home web addresses)**
  - **Mother's maiden name; other names used**
  - **Drug test results and the fact of participation in rehabilitation programs**
  - **Family data**
  - **Religion, race, national origin**
  - **Performance ratings, negotiation of orders**
  - **Names of employees who hold government-issued travel cards, including card data**

WHAT ARE YOUR RESPONSIBILITIES???

- As an employee, you play a very important role in assuring DON complies with the provisions of the Privacy Act. Accordingly,
  - DO NOT collect personal data without authorization
  - DO NOT distribute or release personal information to other employees unless you are convinced they have an official need-to-know

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT be afraid to challenge “anyone” who asks to see PA information for which you are responsible
- DO NOT maintain records longer than permitted
- DO NOT destroy records before disposal requirements are met
- DO NOT place unauthorized documents in PA systems of records

PRIVACY REFRESHER

- Privacy Act provides citizens and lawful aliens with guaranteed rights to:
  - **Access/amend their records, ensuring they are accurate, timely, and complete**
  - **To appeal agency decisions**
  - **To sue for breaches**

PRIVACY REFRESHER

- Privacy Act mandates that:
  - **Agencies may not collect personal data without first publishing a system notice in the Federal Register that announces the collection**
  - **The system notice sets the rules for collecting, using, storing, sharing, and safeguarding personal data**

AS AN EMPLOYEE…

- **You:**
  - **May initiate data collections**
  - **Receive privacy data in the course of conducting business**
  - **Create, manage, or oversee files or databases containing personal data**
  - **And, disseminate personal data**

ACCORDINGLY, YOU HAVE A DUTY TO ENSURE THAT…

- **You receive Privacy Act training**
- **You abide by Privacy Act protocols when collecting, maintaining, destroying, or disseminating personal information**
- **You safeguard personal information**
- **You identify what PA systems notice allows the collection and follows the rulemaking set forth in the notice**

ACCESS TO PERSONAL INFORMATION

- **Do you practice limited access principles?**
  - **Grant access to only those specific employees who require the record to perform specific assigned duties**
  - **You must closely question other individuals who ask for your data**
    - **Why do they need it? How will it be used?**
    - **Is the purpose compatible with the original purpose of the collection?**

REMEMBER…

You can not:

- Initiate new collections of personal data without a covered PA Notice
- Add new elements to an existing and approved data base without a covered PA Notice
- Create or revise forms that collect personal data
- And/or deploy surveys

Without thinking P-R-I-V-A-C-Y !

TRANSMITTING PERSONAL DATA

- **Do not use interoffice mail envelopes to route personal data-use sealable envelopes addressed to the authorized recipient**

- **Properly mark personal data that you transmit via letter or email: “For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties”**

SAFEGUARD PERSONAL DATA

- **Store in an “out-of-sight” location**
- **Do not leave out in open spaces**
- **Take steps to properly destroy data to preclude identity theft**
- **Only share with individuals having an official need to know**
- **Do not lose control of the record**

MAKE PRIVACY A PRIORITY

- Voice your commitment to protecting personal privacy
- Abide by the DON Code of Fair Information principles (individual access, limited collection, retention, use, and disclosure, quality data and safeguarding of data)
- Use caution when posting data to shared drives, multi-access calendars, etc

MAKE PRIVACY A PRIORITY

- **Periodically review shared devices for compliance**
- **If you have a web site, ensure that documents posted therein do not contain personal data**
- **As you move from paper to electronic records, review established practices to determine if they are best practices**
- **Don’t collect personal data because you might need it – collect it because you do need it – what you collect you must protect!**

WHEN PERSONAL DATA IS LOST, STOLEN, OR COMPROMISED…

- **DON seeks to ensure that all personal information is properly protected to preclude identity theft**

- **DEPSECDEF issued a memo on 15 JUL 2005 requiring DOD activities to notify affected individuals within 10 days**
- **Individuals include:**
  - **Military members and retirees**
  - **Civilian employees (appropriated and non-appropriated)**
  - **Family members of a covered individual**
  - **Other individuals affiliated with DOD/DON (e.g., Volunteers)**

PRIVACY TOOL BOX

- WEB SITE: WWW.PRIVACY.NAVY.MIL

  - **Lists all approved Navy and Marine Corps Privacy Act systems of records**
  - **DOD systems and Government-wide systems**
  - **SECNAVINST 5211.5E, DON Privacy Program**
  - **Provides guidance**
  - **Contains training packages**
  - **And so much more!**

FINALLY…

- **You are entrusted with personal information of others. You are the first line of defense in ensuring safeguarding privacy and protecting DON from damaging lawsuits.**

- **FACTOR PRIVACY IN YOUR WORKPLACE!!!**

- **Please direct any questions to your command Privacy Officer Mr. Dave German, (PERS-00J6), 874-3165 or E-mail: DAVID.GERMAN@NAVY.MIL**

NAVY PERSONNEL COMMAND PRIVACY ACT DOCUMENTS POLICY

- Web Site for Article 0130-040 CH-1: https://www.npc.navy.mil/NR/rdonlyres/F974C3E3-5D49-4F27-A908-A3E09D00E920/0/0130040CH1.doc

- NAVPERSCOMINST 5000.1,
  Article 0130-040 CH-1 provides guidance for the disposition of records and files.
- All documents that contain PA information shall be shredded prior to placing in the paper-recycling areas.

RECORDS DISPOSITION

- Web Site For Records Manual: http://doni.daps.dla.mil/SECNAV%20Manuals1/5210.1.pdf

- Must ensure no unnecessary files are created or maintained.
- Navy Records Management Manual provides schedules of retention for files.
- If in doubt as to disposition of files, contact Records Officer (PERS-332) Extension 4-3059.

NAVPERSCOM RECORDS

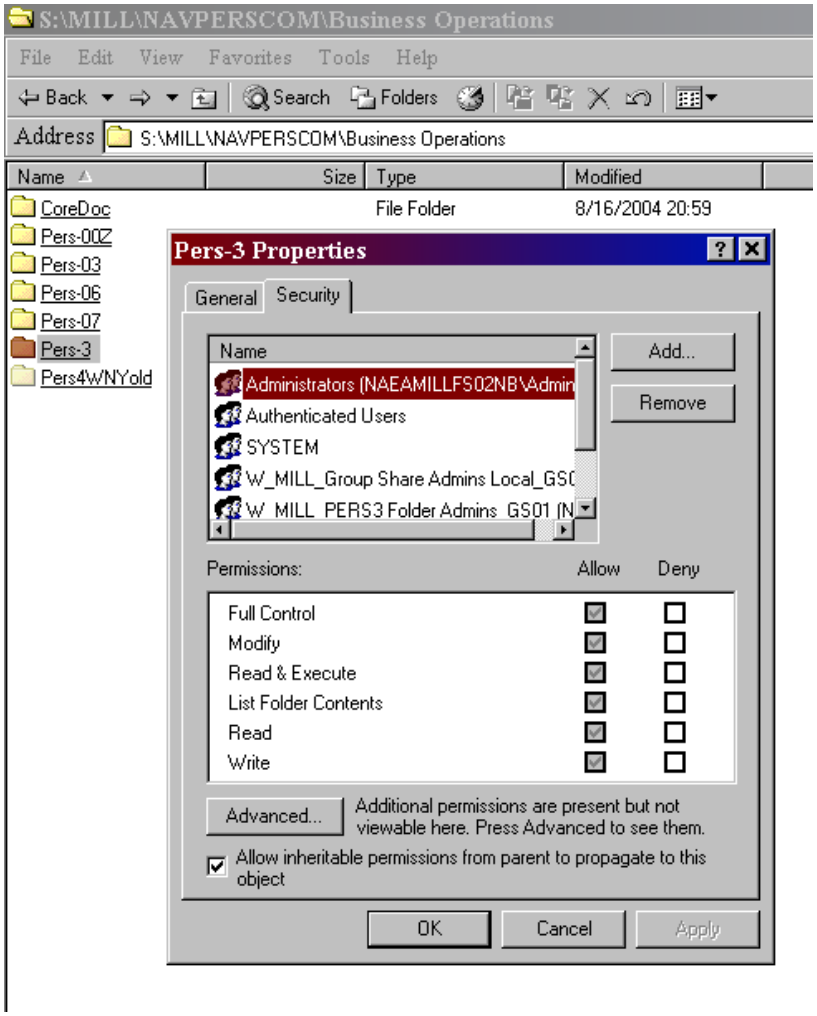
- RECORDS DISPOSAL SCHEDULES ARE ASSIGN BY SSIC. **(STANDARD SUBJECT IDENTIFICATION CODES.)**
- **TYPES OF NAVPERSCOM RECORDS:**
  - **1000-1099 GENERAL MILITARY PERSONNEL RECORDS.**
  - **1300-1399 ASSIGNMENT & DISTRIBUTION RECORDS**
  - **1400-1499 PROMOTION & ADVANCEMENT RECORDS.**
  - **1700-1799 MORALE & PERSONNEL AFFAIRS RECORDS**
  - **1800-1999 RETIREMENTS & SEPARATION RECORDS.**
  - **4000-4999 LOGISTIC RECORDS.**
  - **7000-7999 FINANCIAL MANAGEMENT RECORDS.**
  - **12000-12999 CIVILIAN PERSONNEL RECORDS.**

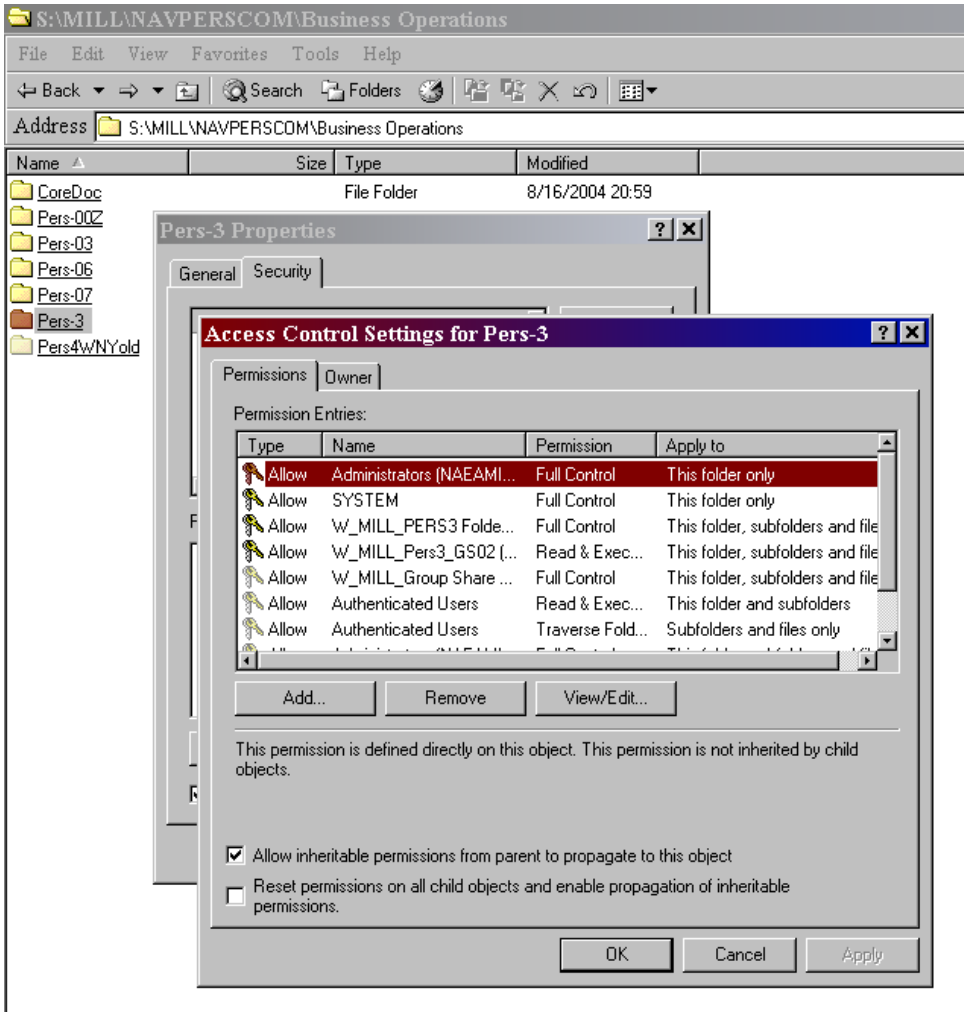
  Most of our records can be disposed of after 2 years or earlier; however, some records that have longer retention requirements are archived at the Washington National Records Center as they have a permanent value to the command. Example: Casualty Records, Directives, MILPERSMAN, etc.

Electronic Files/Folders Containing Privacy Act Data

- **Protect all files and folders on networked shared drives – SIPRNET, NMCI, Legacy**
- **For all sensitive information – Classified (SIPRNET Only), Privacy Act, FOUO, Proprietary, etc.**
- **User responsibilities for managing File/Folder access:**
  - **Password for documents, spreadsheets, databases, etc.**
  - **File naming conventions: avoid using SSN as part of the filename**
  - **Mark privacy records (files, reports) appropriately with "For Official Use Only – Privacy Act Sensitive"**
  - **Web access – remember public/private spaces when publishing to WCMS, i.e., no SSN's on public web sites**
- **Questions on file/folder security management can be answered by your department IAO.**

Folder Security Permissions




S:\MILL\NAVPERSCOM\Business Operations
File Edit View Favorites Tools Help
Back Search Folders
Address S:\MILL\NAVPERSCOM\Business Operations
Name Size Type Modified
CoreDoc File Folder 8/16/2004 20:59
Pers-00Z
Pers-03
Pers-06
Pers-07
Pers-3
Pers4WNYold
Pers-3 Properties
General Security
Access Control Settings for Pers-3
Permissions Owner
Permission Entries:
Type Name Permission Apply to
Allow Administrators (NAEAMI... Full Control This folder only
Allow SYSTEM Full Control This folder only
Allow W_MILL_PERS3 Folde... Full Control This folder, subfolders and file
Allow W_MILL_Pers3_GS02 (... Read & Exec... This folder, subfolders and file
Allow W_MILL_Group Share ... Full Control This folder, subfolders and file
Allow Authenticated Users Read & Exec... This folder and subfolders
Allow Authenticated Users Traverse Fold... Subfolders and files only
Add... Remove View/Edit...
This permission is defined directly on this object. This permission is not inherited by child objects.
Allow inheritable permissions from parent to propagate to this object
Reset permissions on all child objects and enable propagation of inheritable permissions.
OK Cancel Apply

WHAT SPECIFIC ACTIONS ARE EXPECTED OF YOU?

- Avoid using privacy information unless absolutely necessary
- Purge records in accordance with the Navy Records Management Manual
- Shred paper records containing privacy information when disposing
- Mark records, including emails, containing privacy information: “For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil or criminal penalties”

QUESTIONS?

THANK YOU FOR ATTENDING PRIVACY TRAINING